Securing IoT Using Lightweight Cryptography: A Review

Prof. Pravina Parmar[1] Prof. Avani Patel[2] Prof. Sonal Bhavsar[3] Prof. Deepali Jain[4]
[1,2,3,4]Assistant Professor
[1,2,3,4]Department of Computer Engineering & Information Technology
[1,2,3,4]LDRP-ITR, Gandhinagar, India

Abstract— The Internet of Things (IoT) has transformed the way we live and work by connecting billions of devices to the internet, creating a highly interconnected and data-driven ecosystem. However, the rapid proliferation of IoT devices has introduced significant security challenges, as many of these devices operate with resource-constrained hardware, making them vulnerable to cyberattacks. This paper explores the critical need for robust security measures in the IoT landscape and presents a solution in the form of Lightweight Cryptography (LWC).Traditional cryptographic techniques are often too computationally intensive and memory-consuming for IoT devices with limited processing power and memory. Lightweight Cryptography offers a tailored approach to address these constraints while ensuring the confidentiality, integrity, and authenticity of data exchanged between IoT devices and systems. In this paper, we delve into the fundamental principles of Lightweight Cryptography and its suitability for IoT security. We examine various lightweight cryptographic algorithms, and discuss their advantages in terms of efficiency and security. We also highlight the importance of key management and secure communication protocols in IoT security. Furthermore, we explore practical use cases where Lightweight Cryptography can be implemented to enhance the security of IoT applications, including smart homes, industrial automation, healthcare, and transportation systems. By adopting lightweight cryptographic techniques, IoT ecosystems can mitigate security threats, protect sensitive data, and ensure the long-term sustainability and reliability of IoT deployments. In an era where IoT continues to reshape our world, securing this interconnected landscape is imperative, and Lightweight Cryptography emerges as a promising solution to safeguard the future of IoT.

Key words: Lightweight Cryptography, IoT Security, Resource Constrained Devices, Internet Of Things, Elliptic Curve Cryptography (ECC), Lightweight Cryptographic Hash Function, Lightweight Encryption

I. INTRODUCTION

IoT stands for "Internet of Things." It refers to a network of physical objects or "things" that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. These objects can be everyday items like appliances, vehicles, wearable devices, industrial machines, and more.

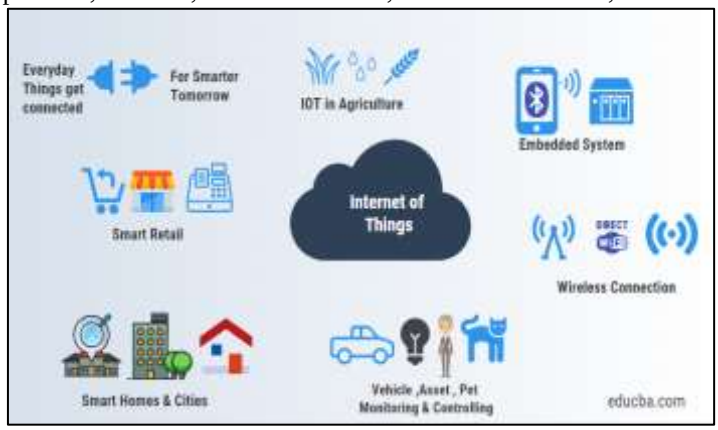

Fig. 1: Internet of Things [28]

The main idea behind IoT is to enable these objects to collect and transmit data, interact with their environment, and sometimes even make autonomous decisions, all without requiring direct human intervention. This data can be used for various purposes, including monitoring and control, automation, data analysis, and improving efficiency and convenience in various aspects of our lives.

IoT has applications in a wide range of industries, including smart homes, healthcare, agriculture, manufacturing, transportation, and smart cities, among others. The proliferation of IoT devices has the potential to revolutionize how we live and work by making our environments more interconnected and intelligent. However, it also raises concerns about privacy, security, and the responsible use of data.

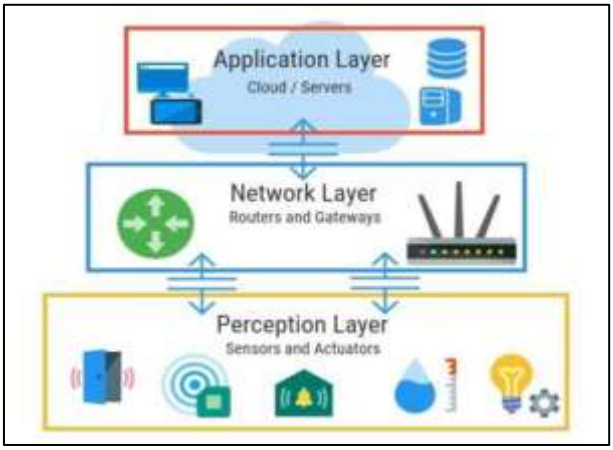

Fig. 2: Three Fundamental layers of IOT [29]

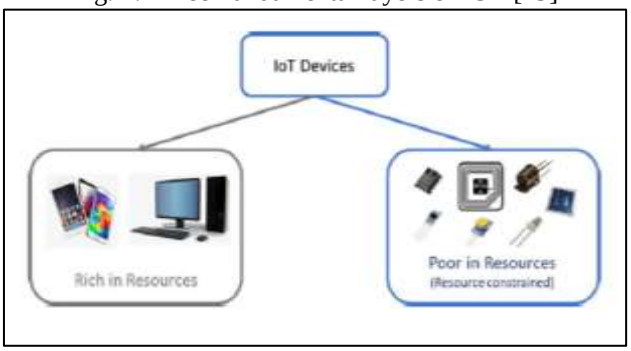

Fig. 3: Two main categories of IoT Devices[1]

A. Lightweight cryptography

Lightweight cryptography refers to cryptographic algorithms and protocols that are specifically designed to be efficient and resource-friendly, making them suitable for use in resource-constrained environments, such as low-power devices, embedded systems, and IoT (Internet of Things) devices. These lightweight algorithms aim to provide a reasonable level of security while minimizing the computational, memory, and energy requirements.

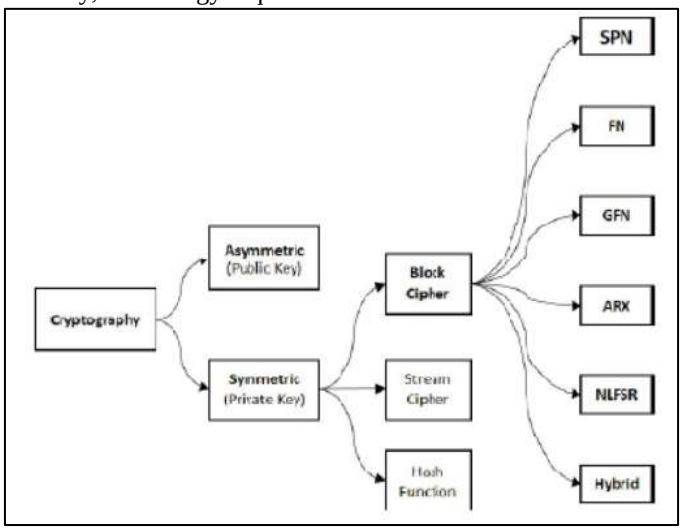

Fig. 4: Structure wise Classification of LWC [1]

Some key characteristics of lightweight cryptography include:

1) Low Resource Usage: Lightweight cryptographic algorithms are designed to have a small code size and require minimal memory and processing power. This makes them suitable for devices with limited hardware capabilities.
2) Efficient Performance: Lightweight ciphers and hash functions are optimized for fast encryption and decryption operations. They are typically designed to minimize latency and energy consumption.
3) Security: While lightweight cryptography prioritizes efficiency, it also aims to provide a sufficient level of security for the intended application. This means that the algorithms should resist common cryptographic attacks.
4) Compactness: Lightweight cryptographic algorithms aim to minimize the size of the cryptographic keys and data structures used in the encryption and authentication processes.

5) Resistance to Side-Channel Attacks: Lightweight ciphers often take into account the vulnerability of small devices to side-channel attacks, such as power analysis and timing attacks. They may incorporate countermeasures to mitigate these risks.
6) Examples of lightweight cryptographic algorithms include lightweight block ciphers (e.g., PRESENT, Clefia), lightweight hash functions (e.g., Keccak, BLAKE2), and lightweight authentication protocols (e.g., HMAC-based Lightweight Protocols).
7) Lightweight cryptography is important because many IoT devices and embedded systems operate in resource-constrained environments and require cryptographic protection for data confidentiality, integrity, and authentication. Using heavyweight cryptographic algorithms in such scenarios can be impractical due to their high resource demands. Therefore, lightweight cryptography plays a crucial role in securing these devices while maintaining their efficiency and functionality. However, it's important to choose lightweight algorithms carefully, considering the specific requirements and threat models of the application in question to ensure adequate security.

II. LITERATURE REVIEW

In 2021 Vishal A. Thakor, Mohammad Abdur Razzaqueet al.[1]had worked on review comparison and research opportunities in lightweight cryptography for resource constrained devices.The paper commences with an overview of the IoT landscape, highlighting the diverse range of IoT applications across industries, emphasizing the need for cryptographic security measures. It underscores that traditional cryptographic algorithms are often impractical for IoT devices due to their limited computational power, memory, and energy resources.

The core of the paper consists of a thorough review and comparison of various lightweight cryptography algorithms, such as SIMON, Speck, HIGHT, and others. Each algorithm's design principles, security features, and performance characteristics are analysed, providing a clear understanding of their suitability for IoT applications. Additionally, the paper assesses their resistance to common cryptographic attacks and explores their adaptability to the IoT environment.

The research paper goes beyond a mere comparison by identifying emerging trends and research opportunities in the field of lightweight cryptography for IoT. It discusses potential enhancements to existing algorithms, the exploration of new cryptographic primitives, and innovative approaches to key management and secure communication protocols. Moreover, it emphasizes the importance of standardization efforts in promoting interoperability and security in the IoT ecosystem.The authors acknowledge the trade-offs between security and resource constraints in IoT and suggest that a one-size-fits-all approach may not be suitable. Instead, they advocate for a nuanced approach where the choice of lightweight cryptography algorithm depends on the specific requirements and threat models of the IoT application.

In conclusion, The well-defined LWC characteristics(cost, performance and security) by NIST are compared, andfurther research gaps and open research challenges are highlightedin this paper. From the literature review, PRESENTand CLEFIA are the approved block ciphers by NIST due tosecurity reasons along with accepted performance and cost. On the other side, SIMON and SPECK impress by theirmost compact implementations. In general, none of the LWCalgorithms fulfils all the criteria of hardware and softwareperformance metrics but performs at their best in the specifiedenvironment. However, new attacks are reported with thegrowth of new LWC algorithms which is an inevitable andnever-ending process. The war between cybersecurity expertsand attackers always opens a door of opportunities for newresearch in the field of cybersecurity, especially lightweightcryptography.

Ayoub Mhaouch, Riadh Ayachi, and others [2] worked on network-on-a-chip data encryption in 2021.Using lightweight cryptographic algorithms to secure data in Network-on-Chip (NoC) architectures is the main emphasis of the research project.

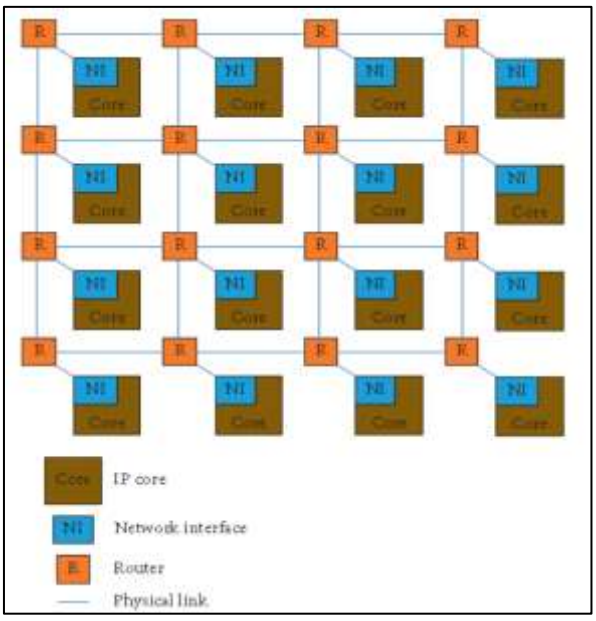

Fig. 5: Typical architecture of NoC [2]

Given their resource limitations and requirements for real-time data transfer, it examines the necessity of effective encryption techniques in NoCs. The article addresses the difficulties in integrating conventional cryptographic algorithms into network operating systems (NoCs) and suggests lightweight cryptography as a workable remedy. Additionally, it offers information about particular lightweight encryption methods and how well they function in NoC settings.
This paper's primary contributions are as follows:

1) Offering a NoC NI with excellent performance and security
2) Putting forth a NoC-based, low-power encryption algorithm based on the LED64 algorithm
3) To prevent data waiting and shorten processing times, suggest a larger input/output FIFO.
4) Using the XilinxVirtex 5 XC5VFX200T to synthesize the suggested solution
5) A tiny footprint and fast processing speed are combined to produce high performance.
6) Ensuring that the suggested NI with limited resources devices are used.

In summary, the increasing amount of embedded IPs in developing technologies is straining SoCs to their breaking point. NoCs were thought to be the answer to achieving flawless, non-overlapping IP connectivity, enabling the usage of common buses, and minimizing connecting cables. The router, network links, and network interface (NI) are the three primary parts of NoC. The NI is thought to be the most crucial element in arranging the sending and receiving of data. To protect data, we suggested an NI design with a thin block cipher in this work. The suggested NI was meant to work with any NoC. To prevent data waiting, a large input/output FIFO is used. Because of its high level of security, quick processing speed, and little implementation area, the LED block cipher was employed to encrypt data. According to the published data, the suggested NI design performs better than previous efforts that use the AES block cipher and have a wide range of implementation areas and operating frequencies. The suggested architecture is more suited for usage on IoT devices and other devices with constrained computational resources.

In 2022,Hakeem Imad Mhaibes, May Hattim et al. [3] worked on Simple Lightweight Cryptographic Algorithm to Secure Embedded IoT Devices that presents a new cryptographic algorithm specifically designed to enhance the security of embedded Internet of Things (IoT) devices. In summary, the paper introduces a novel cryptographic algorithm tailored for IoT devices, offering a simplified yet effective approach to securing embedded IoT devices in an increasingly interconnected world. Generally, symmetric cryptography uses same key for encryption and decryption. Since the proposed modified TEA used 32 keys, that is one key for each round and numbered such as [$KK0$, $KK1$, $KK2$, . . . $KK31$]. For decryption part, keys are in reverse order, such as, $KK31$ is used for the first round and $KK30$ for second round and so on.

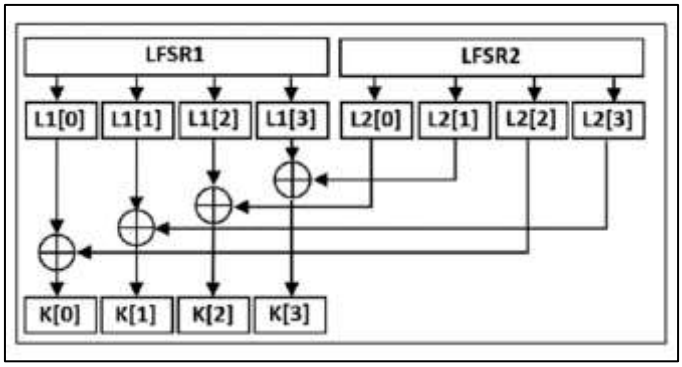

Fig. 6: New proposed keys generation [3]

III. RESULT AND ANALYSIS:

Three crucial security analysis criteria for block ciphers—the key sensitivity, completeness, and avalanche effect tests are used to gauge the proposed algorithm's security strength. These experiments demonstrate that the modified TEA algorithm offers greater security strength when compared to the standard TEA method.

This paper intended to increase the security performance of the original TEA. The modification offers a simple and a new modified method of key generation using two LFSRs. The security vulnerability of the original TEA was solved. The encryption and decryption performance of modified TEA was analyzed using key sensitivity, avalanche effect, and completeness test to be compared with the previous work of traditional TEA and MTEA.

- Through key sensitivity analysis evaluation, the proposed implementation of new key generation for modified TEA could generate keys that have higher randomness characteristic and more confusion than other.
- For completeness test, 65 plaintexts were tested, where there is only one-bit variation between each plaintext and the one after it. This test is run on both the modified and original TEA. The results indicate that, proposed method achieves highest completeness test, which means that, when one bit change in the plaintext, the output ciphertext changes significantly. This property is desirable for security analysis of the cryptographic algorithm.
- Moreover, modified TEA has higher value of avalanche effect. This test proved that, 50 % or higher of ciphertext is will be changed if one bit or few bits of the plaintext changed. For avalanche effect, the minimum value of margin is 2.48 and the maximum is 6.89 for 10 tested blocks. The benchmark created for differentiate the modified TEA to original TEA. Evidently, the proposed method exceeded the typical threshold of 50 percent for avalanche effect processes. Since embedded IoT devices are resource constraint, the modified work is simple and has no complexity overhead. In addition,

LFSR is a simple and an appropriate way to use in such devices because of its simplicity computation. Therefore, the proposed work is suitable for latest IoT applications to transfer data through network.

By encrypting the compressed file, the modified TEA would be used. Also, future plans include implementing and integrating this technique in fog net, sensor, or ad hoc for data transmission.

Muhammad Rana, Quazi Mamun, et al.'s 2022 report [4] offers a thorough analysis of the use of lightweight cryptography methods in Internet of Things (IoT) networks. The most recent cutting-edge research in lightweight cryptography for 2019 and 2020 is covered in this paper. A comparative analysis of the majority of the most recent lightweight algorithms, including SAT_Jo, LCC, LWHC, and Modified PRESENT, is also presented.

IT uses a set of matrices, including block size, key length, gate area, technology value, number of encryptions or decryptions, latency, and throughput, to assess the most recent protocols.

Focuses on the subsequent inquiries:

1) What kind of lightweight cryptography has been created to solve the security problems with IoT?
2) How can an IoT structure be secured using lightweight cryptography?
3) How do the results affect the direction of IoT research going forward?

Discussed about the different potential attacks on IoT's architectural layers.

Attacks at the application layer and security layer include phishing, buffer overflow, cross-site scripting, SQL injection, denial-of-service, and data privacy concerns.

Attacks against the middleware layer and security include those against applications, data, replay, sleep deprivation, and unauthorized access.

Attacks on the network layer and security, such as eavesdropping, device cloning, spoofing, DDoS, traffic analysis, brute-force, man-in-the-middle, and sinkhole.

IoT layer architecture and task.

Layer	Component	Tasks
Application layer	Third-party application, consoles, websites, touch panel.	Machine learning, business model, graphs and flowcharts.
Middleware layer	Vendor-specific third-party application.	Machine learning, processing, pre-processing, and real-time action.
Network layer	Nodes, gateways, firmware.	Transmit and process data, device management, process and secure routing.
Perception layer	Sensors (temperature and humidity), actuators (relays and motor).	Transfer data, identity, monitor, acquisition and action.

Table 1: IoT architecture layers, components and tasks [4]

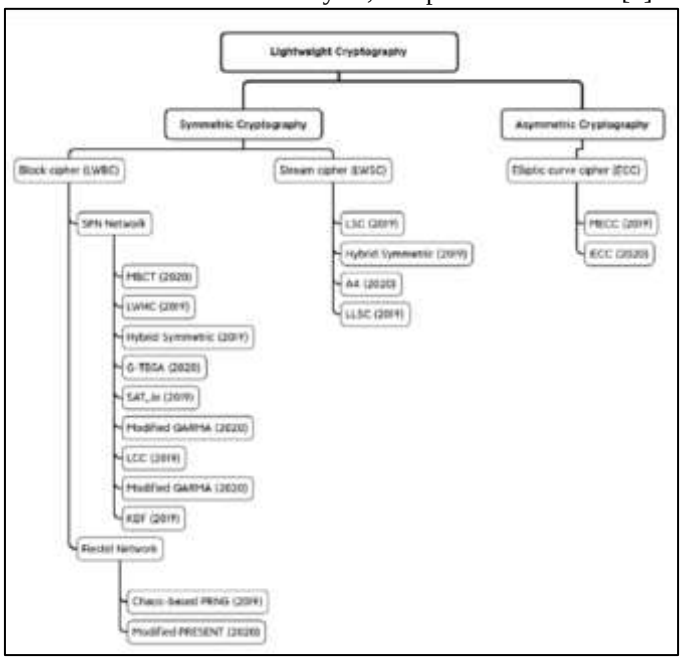

Fig. 7: Classification of recently developed lightweight cryptography algorithms [4]

It covers lightweight algorithms for IoT network security in a clear and concise manner. Moreover, categorizes the most recent advancements in lightweight algorithms. The article provides examples of various forms of modern lightweight cryptography, which can be categorized into two groups: symmetric and asymmetric algorithms. Lightweight Block Ciphers (LWBC) and Lightweight Stream Ciphers (LWSC) are two more categories into which the symmetric lightweight algorithms

are separated. Asymmetric cryptography includes elliptic curve cryptography (ECC). A lightweight cryptographic primitive's factors are determined by the number of rounds, structures, block size, and key size. Also covered was the recent advancement of three cipher technologies—block, stream, and elliptic curve ciphers—that are used to safeguard Internet of Things networks with limited resources.

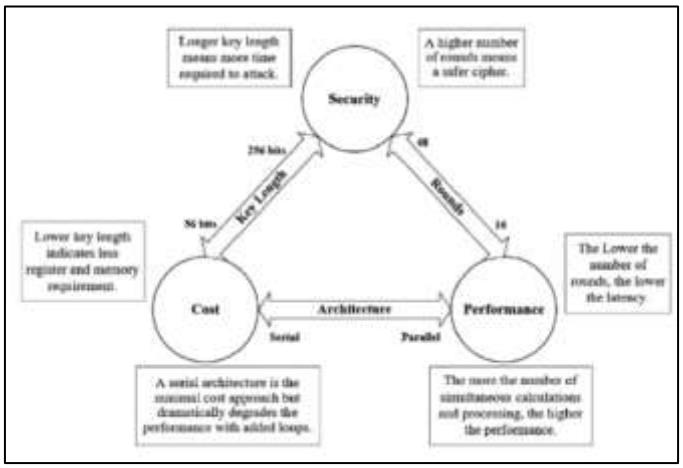

Fig. 8: Trade-off between cost, performance, and security. [4]

The challenges of a lightweight block cipher

- Create a sturdy P-box and S-box.
- Use a key that is shorter.
- Create a straightforward key structure.
- Produce an algorithm with fewer and simpler rounds.
- Make greater use of dynamic keys.
- Use a more manageable data block.

Problems with the lightweight stream cipher include:

- Using a smaller key.
- Diminish the interior condition.
- Limit the area of the chip.

In order to maintain the security of data communication, current research on lightweight cryptography techniques is examined. Regarding maintaining security while exchanging data in the Internet of Things context, each algorithm has advantages and disadvantages. Certain algorithms require less computing power but require more storage, and vice versa. Many algorithms are efficient in terms of energy, computing power, and cost, but they are not resistant to different kinds of attacks. Block ciphers and stream ciphers are two popular recently developed symmetric algorithms used in IoT security; however, neither of these is ideal for securing resource-constrained communications in IoT systems. One crucial issue with the Internet of Things is security, which has not received enough attention in the most recent network security research. It is necessary to create a lightweight cryptographic algorithm to safeguard IoT architecture with limited resources. There is a need for research on improving lightweight ciphers due to the increasing attack patterns on IoT networks. In order to develop lightweight block ciphers, future research could benefit from concentrating on reducing key size, using a more frequent dynamic key, decreasing block size, introducing more straightforward rounds, and creating simple key schedules. Develop future lightweight stream ciphers with internal state, key size minimization, and vector initialization as top priorities.

A novel cryptographic algorithm is introduced in 2022 by Lo'aiTawalbeh, Michael Alicea, et al. [5] with the goal of improving the security of web and mobile applications. The algorithm specifically addresses the need for effective encryption techniques. As part of the testing for this project, this paper focuses on the three lightweight cryptography algorithms: TWINE, PRESENT, and PRINCE.

A. PRINCE

A portable crypto algorithm known as the PRINCE block cipher was unveiled in 2012. 64 bit blocks and a 128 bit key are used in the Prince cipher. Key expansion to 192 bits is the first action taken by PRINCE. To accomplish this, divide the key in half, creating the 64-bit keys k0 and k1. During the cipher rounds, the half of the key indicated by the symbol k1 is used. The value of a bit-wise shift of k0 and the value of a cyclic shift of k0 are then XORed to create a k'0. The concatenation of k0, k'0, and k1 yields the entire 192-bit expanded key. PRINCE proceeds to its 12-round process of substitutions and permutations after key expansion.

Every stage comprises the subsequent actions:

- Every round, the cipher substitutes using an S-Box. This S-Box replaces 4 bits with another 4 bits.
- RC0 through RC11 are the 12 predefined round constants used in the cipher. Each of these constants is used during the corresponding round by means of an iteration process. The round constant for that round is XORed with the state at that moment.

The current state is multiplied by the matrix M in a linear layer. This matrix represents the state with shift rows applied in the AES style. The middle round, when the state is multiplied by M1, is the exception.

The PRINCE cipher aims to provide reasonably strong encryption at an affordable price so that devices with lower security levels can still benefit from a moderate level of protection.

B. PRESENT

The 31-round process is used by the PRESENT cipher in the following manner:

each round of the process involves an XOR with a subset of the key and the data's current state; the PRESENT cipher uses a 4 bit to 4 bit S-Box to substitute bits in both the round key and the state of every round. The 64 bits on the left side of the key are used to XOR the data, rather than using the entire key each round. The first four bits on the left of the key are run through the S-Box after the key is moved 61 to the left at the end of each round.

– The data is passed through a P-Box or a permutation box as the final step in each of the 31 rounds. Every round, this P-Box is used to shuffle the block's pieces. In contrast to PRINCE, which executes a cyclic shift, the data is utterly jumbled and devoid of any meaningful pattern.

C. TWINE

The 36-round TWINE cipher process has the following characteristics:

TWINE uses a 4 bit to 4 bit S Box, just like the other ciphers. There are two sections to the key schedule. First, the round key is subjected to the S-Box, causing the key to shift between rounds. Second, the key is subjected to a left cyclic shift using the around constant. TWINE, like PRESENT, chooses not to apply a cyclic shift to the data on rounds. Rather, each round's data state is subjected to what they refer to as a block shuffle.

D. MYPHER

Mypher is a brand-new cipher that is made by combining the features of the ciphers mentioned above. Mypher is a 64-bit block cipher with an 80-bit key that follows the same rules as the ciphers from the previous section. This cipher is a low-cost, light-weight crypto algorithm that aims to offer moderate security. It is best suited for use with Internet of Things devices that send tiny amounts of data periodically, like sensors. The Python programming language was used to write the implementation for this paper.

There is discussion of the Key Cycle, Substitution Box, Permutation Box, and Encryption and Decryption Process of the Mypher. Algorithms are tested using performance tests, key sizes, block sizes, and the environment.
In conclusion, the relative performance of each algorithm was determined using the python implementations of those algorithms. Compared to the current algorithms, Mypher was found to perform similarly on both the Raspberry Pi 3 and 4.

Raspberry Pi 3	Encryption	Decryption
Mypher	4.17118s	5.32321s
Twine	4.154831s	6.44118s
PRINCE	156.96444s	157.22997s
PRESENT	5.79016s	5.78759s
Raspberry Pi 4	Encryption	Decryption
Mypher	1.45062s	1.83058s
Twine	1.50299s	2.38576s
PRINCE	71.47251s	71.65946s
PRESENT	2.03991s	2.02709s
Core i7	Encryption	Decryption
Mypher	0.29653s	0.37770s
Twine	0.27602s	0.42392s
PRINCE	13.68296s	13.65142s
PRESENT	0.37993s	0.39156s

Table 2: ThePerformanceTestResultsUsingRaspberryPi3, RaspberryPi4, and Corei7 [5]

They were able to pinpoint important factors that explained why algorithms operated as they did and the distinctions between the encryption and decryption processes through this testing and code comparison. It was also discovered that performance can vary greatly even amongst Internet of Things devices. This demonstrates that, even for devices with limited resources, there is no one-size-fits-all method for choosing an algorithm. Mohammed El-hajj, Hussien Mousawi, and others have contributed in 2023 [6]. The primary contribution of this effort was to test and compare low-power symmetric ciphers for devices with limited resources. Two popular platforms are employed for the evaluation: Arduino and Raspberry Pi. In the first section, they used the Arduino platform and the Raspberry Pi to create 39 block ciphers on an ATMEGA328p microcontroller. For varying block and key sizes, the block cipher implementations were examined in terms of encryption and decryption speed, cost, and energy efficiency. In the second section, the first-part ciphers were combined with the 80 stream and block cipher algorithms from the second round of NIST candidates. A thorough study was conducted to determine the equivalent block and key sizes in terms of latency and energy efficiency for both encryption and decryption utilizing the two

boards. The speed, the area, and the energy consumption are taken into account for hardware implementation. The necessary memory size (ROM and RAM) of the embedded program is taken into account for software implementation.

By assessing the cryptographic algorithms' performance using a number of metrics and test scenarios to make sure the chosen algorithms are appropriate for usage in a broad range of IoT devices, the work is thought to be unique up to this point. The evaluation procedure considers elements like the performance on various devices. In this research, the widely-used Arduino and Raspberry Pi platforms were utilized to assess and benchmark a collection of 122 ciphers.Among the 122 compared algorithms, LEA-128-128, COMET-64_CHAM-64-128, Hight-64-128, Speck-48-72, Speck-64-128, and XTEA-64-128 showed the most promising in terms of power, speed, and ROM measurements. The top-performing ciphers among the NIST finalists chosen on March 29, 2021, are also Schwaemm-256-128, GIFT-COFB-128-128, Schwaemm-128-128, Xoodyak-128-128, TinyJAMBU-192-32-192, and TinyJAMBU-128-32- 128.

The following features can be viewed as recommendations for future work or as additions and enhancements of this work.

1) An Arduino Mega could be taken into account when analysing methods that use more memory than the ATMEGA328P UNO can accommodate.
2) The key schedule, ROM, RAM, and code size of the NIST finalists between UNO and Pi were not compared; however, these comparisons could be done in the future.
3) The research could include hash function algorithms and stream ciphers.
4) A linear approach was assumed when using the AES as a relative reference. After conducting sufficient research in this area and taking into account the behaviour of the selected algorithms, it might be established as future work using a different method or approximation.
5) It is crucial to remember that ambient variables, like the Pi/UNO's temperature, might also have an impact on the algorithm's effectiveness. Therefore, in future studies, this element should also be taken into account while conducting performance analyses.

In 2023, Nahla Ibrahim and Johnson Agbinya[7] have worked on Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices.

"Small Lightweight Cryptographic Algorithm (SLA)" is proposed. The SLA relies on substitution–permutation network (SPN). It utilizes 64-bit plaintext and supports a key length of 80/128-bits. Compared to other currently used ciphers, SLA has a higher throughput. SLA's performance as an ultra-lightweight compact cipher, and its security analysis is also demonstrated. The SLA cipher's design is well suited for applications where small-scale embedded system dissipation is critical. The SLA algorithm is implemented using Python.

The properties related to the nonlinear and linear components to design SP network structure are exploited.

As they designed the SLA, they researched the minimal numbers of active S-boxes and good S-boxes. They also researched the hamming weight calculation for LAT and DDT entries. The proposed SLA design has achieved a small execution time, high throughput, and high level of security. This makes it suitable for small-scale embedded environments such as RFID tags and wireless sensor nodes. Advanced attacks can be used to examine the SLA scheme further. We expect our results to be applied in other domains as well.

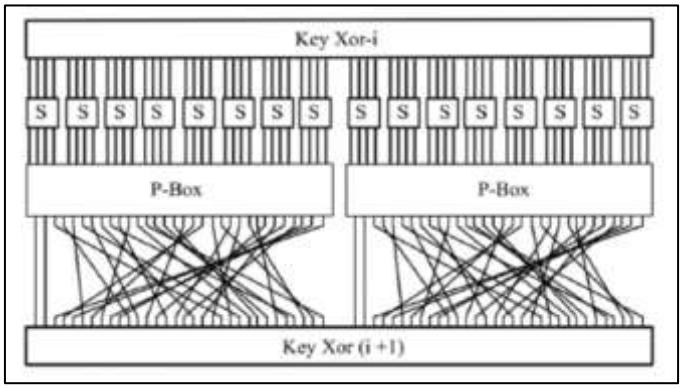

Fig. 9: SLA Block cipher

In 2023 Nam, Tran Sy, Hoang Van Thuc et al. [8] worked on Hardware Architecture of NIST Lightweight Cryptography Applied in IPSec to Secure High-Throughput Low-Latency IoT Networks. They proposed a hardware architecture for Ascon, a NIST Lightweight cryptography standard to enable high-throughput, low-latency security services in IPSec protocols. Results show that the ESP protocol can achieve a maximum throughput of 8.806 Gbps and a minimum latency of 427ns for only 2812 SliceThis ESP core together with the proposed Ascon implementation can be used in IoT gateways to provide security services for high-speed, low-latency IoT

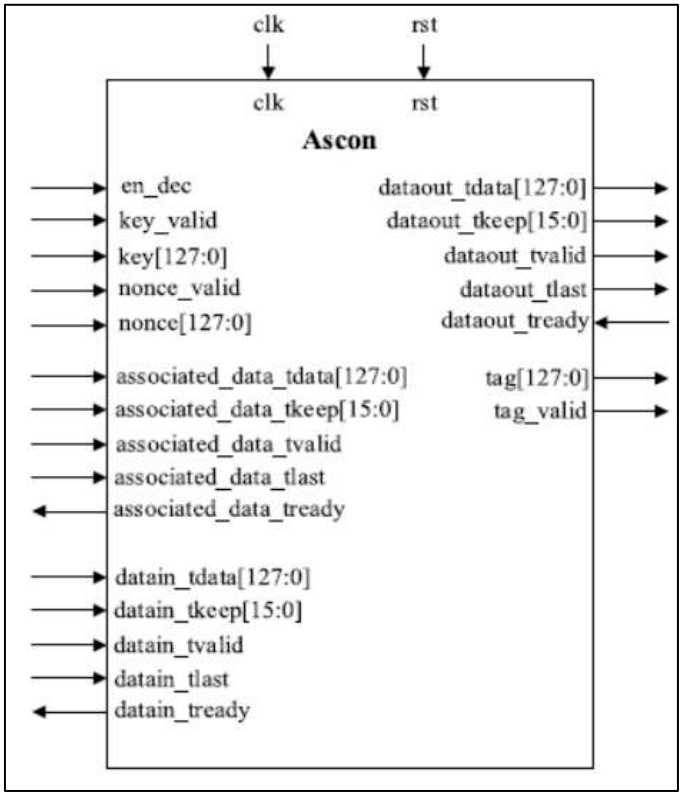

Fig. 10: Ascon interface [8]

Additionally, they present the implementation and evaluation of the IPSec ESP protocol using this architecture in FPGA. All ESP processes and cryptographic algorithms are performed in hardware to achieve high performance with little overhead.

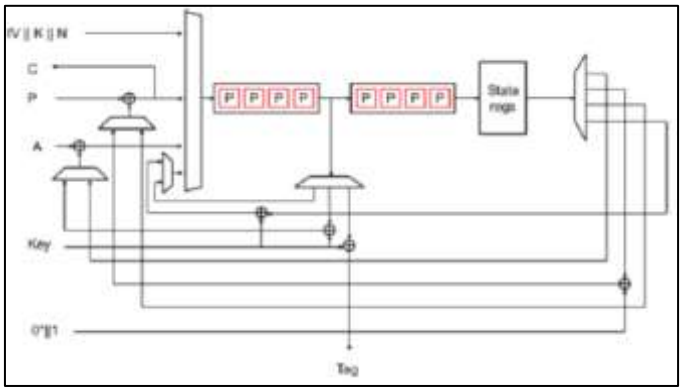

Fig. 11: Ascon-128a hardware architecture [8]

In conclusion The Ascon architecture and IPSec protocol implementation presented in this paper can help address the need for secure, high-speed, low-latency communication in emerging IoT networks.

In future the lowpower consumption of the Ascon and IPsec hardware architecture can be addressed.

In 2022, Tsantikidou, Kyriaki, and Nicolas Sklavos [9] have done the analysis of Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare.In their work renowned lightweight cryptographic primitives and their most recent architecture, are investigated.

Their security, architecture characteristics and overall hardware limitations are analyzed and collected in tables. Finally, all the algorithms are compared based on their effectiveness in securing healthcare applications, the utilized device and the overall implementation efficiency.

Four algorithms were deemed better suited for IoT devices in healthcare applications. These algorithms were the KASUMI block cipher, PRESENT block cipher, Trivium stream cipher and PHOTON-80 hash function.

this paper presented an analysis of the IoT-based healthcare design and the research conducted to date on hardware implementations of cryptographic algorithms. Specifically, the capabilities, to date, and therefore limitations of IoT-based health applications based on the hardware designs of lightweight cryptographic primitives were demonstrated.

For future directions, these conclusions will be considered with the aspirations of improving and simplifying IoT-based implementations for security purposes in the healthcare domain.

In 2023, Rajesh, S. M., and R. Prabha [10] Addressed the Security Issues in Intelligent Applications using Lightweight Cryptographic Approach.

This paper carried out exhaustive work on user/device identity and a lightweight cryptographic viablesolution for the IoT ecosystem through ECC (Elliptic-curve cryptography).

The outcome of this study is essential components of ECC, requirements, and solution architecture of ECC for various security aspects in the IoT ecosystem to ensure user/device privacy and secured data transmission and its challenges are addressed.

A comprehensive study of the research works and its comparison with critical discussion are represented.

To enlighten the future study, the challenges of ECC are discussed with which one can select an appropriate ECC-based technique for securing data in the IoT ecosystem by preserving the user/device privacy.

IV. CONCLUSION

The use of lightweight cryptography algorithms, tailored to the resource constraints of IoT devices, is essential for ensuring data confidentiality, integrity, and authenticity without imposing undue computational burdens.

These algorithms, such as ECC (Elliptic Curve Cryptography), AES (Advanced Encryption Standard), and others, offer efficient cryptographic solutions that strike a balance between security and resource efficiency.However, the choice of algorithm should be made judiciously, taking into account factors like the device's computational capabilities, memory constraints, and communication bandwidth. The diversity of IoT devices and applications necessitates a flexible approach to algorithm selection.

In summary, lightweight cryptography with various algorithms is a cornerstone of IoT security, offering the means to protect sensitive data and ensure the integrity of IoT systems. Yet, a holistic approach to IoT security, encompassing algorithm choice, device management, and ongoing vigilance, is essential to build a resilient defense against the evolving landscape of IoT security threats. As IoT continues to grow and evolve, so too must our security practices to keep pace with the challenges it presents.

REFERENCES

[1] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access*, *9*, 28177-28193.
[2] Ayachi, Riadh, Ayoub Mhaouch, and Abdessalem Ben Abdelali. "Lightweight cryptography for network-on-chip data encryption." *Security and Communication Networks* 2021 (2021): 1-10.
[3] Mhaibes, Hakeem Imad, May Hattim Abood, and Alaa Kadhim Farhan. "Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices." *International Journal of Interactive Mobile Technologies* 16.20 (2022).
[4] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.
[5] Alicea, M., &Alsmadi, I. (2022). New and Efficient Lightweight Cryptography Algorithm for Mobile and Web Applications. *Procedia Computer Science*, *203*, 111-118.
[6] El-Hajj, Mohammed, Hussien Mousawi, and Ahmad Fadlallah. "Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform." *Future Internet* 15.2 (2023): 54.
[7] Ibrahim, Nahla, and Johnson Agbinya. "Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices." *Applied Sciences* 13.7 (2023): 4398.
[8] Nam, Tran Sy, Hoang Van Thuc, and Bui Duy Hieu. "A Hardware Architecture of NIST Lightweight Cryptography applied in IPSec to Secure High-throughput Low-latency IoT Networks." *IEEE Access* (2023).
[9] Tsantikidou, Kyriaki, and Nicolas Sklavos. "Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare." *Cryptography* 6.3 (2022): 45.
[10] Rajesh, S. M., and R. Prabha. "Lightweight Cryptographic Approach to Address the Security Issues in Intelligent Applications: A Survey." *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*. IEEE, 2023.
[11] Windarta, S., Suryadi, S., Ramli, K., Lestari, A. A., Wildan, W., Pranggono, B., &Wardhani, R. W. (2023). Two new lightweight cryptographic hash functions based on saturnin and beetle for the Internet of Things. *IEEE Access*.
[12] Dwivedi, Ashutosh Dhar, and Gautam Srivastava. "Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK." *Internet of Things* 21 (2023): 100677.
[13] Silva, C., Cunha, V. A., Barraca, J. P., & Aguiar, R. L. (2023). Analysis of the Cryptographic Algorithms in IoT Communications. *Information Systems Frontiers*, 1-18.
[14] Ahmed, A. A., Malebary, S. J., Ali, W., & Alzahrani, A. A. (2023). A Provable Secure Cybersecurity Mechanism Based on Combination of Lightweight Cryptography and Authentication for Internet of Things. *Mathematics*, *11*(1), 220.
[15] Parmar Martin, and Parth Shah. "Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application." *International Journal of Electrical and Computer Engineering (IJECE)* 13.4 (2023): 4422-4431.
[16] Shah, Pooja, Mukesh Arora, and Kinjal Adhvaryu. "Lightweight Cryptography Algorithms in IoT-A Study." *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. IEEE, 2020.
[17] Sridhar, S., and S. Smys. "Intelligent security framework for iot devices cryptography based end-to-end security architecture." *2017 International Conference on Inventive Systems and Control (ICISC)*. IEEE, 2017.

[18] Wankhade, Shashank P., and A. N. Bandal. "Security for Automation in Internet of Things Using One Time Password." *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE, 2017.
[19] Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A., &Fartitchou, M. (2020). IoT security: challenges and countermeasures. *Procedia Computer Science*, *177*, 503-508.
[20] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 73-80.
[21] Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications*, *112*, 1947-1980.
[22] Internet of Things research study, accessed on 20-Oct 2016.
[23] HP White paper retrieved in Aug 2015 http://go.saas.hp.com/food/internet of things.
[24] Study of security issues and solutions in Internet of Things (IoT) Shashi Rekha, Lingala Thirupathi , Srikanth Renikunta , Rekha Gangula
[25] Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review
[26] Gunathilake, N. A., Al-Dubai, A., & Buchana, W. J. (2020, November). Recent advances and trends in lightweight cryptography for IoT security. In *2020 16th International Conference on Network and Service Management (CNSM)* (pp. 1-5). IEEE.
[27] Regla, Alfio I., and Enrique D. Festijo. "Performance analysis of light-weight cryptographic algorithms for internet of things (IOT) applications: A systematic review." *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*. IEEE, 2022.
[28] https://www.bisinfotech.com/top-iot-startups-in-india/
[29] https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization